



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/558,942	08/21/2006	Gary Paul Noble	GB920030011US1	7231
45832	7590	03/03/2011	EXAMINER	
DILLON & YUDELL LLP 8911 N. CAPITAL OF TEXAS HWY., SUITE 2110 AUSTIN, TX 78759			SU, SARAH	
			ART UNIT	PAPER NUMBER
			2431	
			NOTIFICATION DATE	DELIVERY MODE
			03/03/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

Patents@DillonYudell.com



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

Application Number: 10/558,942
Filing Date: August 21, 2006
Appellant(s): NOBLE, GARY PAUL

Michael R. Long, Reg. No. 42,808
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 13 December 2010 appealing from the Office action mailed 23 July 2010.

(1) Real Party in Interest

The examiner has no comment on the statement, or lack of statement, identifying by name the real party in interest in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The following is a list of claims that are rejected and pending in the application:

Claims 1-5, 8-12, 16-20, and 22-24 are pending.

Claims 1-5, 8-12, 16-20, and 22-24 are rejected.

(4) Status of Amendments After Final

The examiner has no comment on the appellant's statement of the status of amendments after final rejection contained in the brief.

(5) Summary of Claimed Subject Matter

The examiner has no comment on the summary of claimed subject matter contained in the brief.

(6) Grounds of Rejection to be Reviewed on Appeal

The examiner has no comment on the appellant's statement of the grounds of rejection to be reviewed on appeal. Every ground of rejection set forth in the Office action from which the appeal is taken (as modified by any advisory actions) is being maintained by the examiner except for the grounds of rejection (if any) listed under the subheading "WITHDRAWN REJECTIONS." New grounds of rejection (if any) are provided under the subheading "NEW GROUNDS OF REJECTION."

(7) Claims Appendix

The examiner has no comment on the copy of the appealed claims contained in the Appendix to the appellant's brief.

(8) Evidence Relied Upon

US 6,603,857 B1	Batten-Carew et al.	8-2003
US 6,813,358 B1	Di Crescenzo et al.	11-2004
US 2001/0052071 A1	Kudo et al.	12-2001

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1-5, 9-12, 19, 20, 23, and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Batten-Carew et al. (US Patent 6,603,857 B1) and Batten-Carew hereinafter) in view of Kudo et al. (US 2001/0052071 A1 and Kudo hereinafter).

As to claims 1, 23, and 24, Batten-Carew discloses:

a trusted body generating an asymmetrical key pair for a specified date and time of disclosure with an encryption key and a decryption key
(col. 3, lines 39-47);

the publisher using the encryption key to encrypt data (col. 3, lines 50-51);

the recipient obtaining the encrypted data (col. 3, lines 51-54);
the trusted body making the decryption key available to the recipient at the specified date and time (col. 3, lines 57-61), **wherein the trusted body generates one or more asymmetrical key pairs for the specified date and**

time, generating a new asymmetrical key pair for each of a plurality of publishers (col. 3, lines 44-47).

Batten-Carew fails to specifically disclose:

the trusted body providing a digital certificate signed with a private key of the trusted body to the publisher prior to the specified date and time, the digital certificate providing the publisher with the encryption k prior to the specified date and time;
each of the plurality of publishers has a password issued by the trusted body for preventing disclosure of the decryption key.

Nonetheless, these features are well known in the art and would have been an obvious modification of the teachings disclosed by Batten-Carew, as taught by Kudo.

Kudo discloses a system and method for time-dependent decryption, the system and method having:

the trusted body providing a digital certificate signed with a key of the trusted body to the publisher prior to the specified date and time, the digital certificate providing the publisher with the encryption k prior to the specified date and time (0003, lines 4-10; 0061, lines 10-13; 0065, lines 1-5), but does not explicitly disclose where the digital certificate is signed with a private key.

each of the plurality of publishers has a password issued by the trusted body for preventing disclosure of the decryption key (0003, lines 4-10; 0024, lines 1-5).

It is well known in the art that signed documents in a public-key cryptography system are signed using a private key, as evidenced by Schneier (page 37, lines 26-30; page 185, lines 38-39; page 186, lines 1-7). Therefore, since Kudo discloses that the digital certificate is signed with a key, it is signed with a private key.

Given the teaching of Kudo, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Batten-Carew with the teachings of Kudo by providing an encryption key through a digital certificate prior to a specified time and issuing a password. Kudo recites motivation by disclosing that providing keys in a time-key certificate guarantees that a time for enabling decryption information is limited (0019, lines 1-6). Kudo also discloses that each certificate contains the name of the user used to confirm that the certification authority has provided the digital signature for the public encryption key for that user, guaranteeing that no person other than that user can decrypt the encrypted data (0003, lines 4-10; 0004, lines 4-5). It is obvious that the teachings of Kudo would have improved the teachings of Batten-Carew by providing an encryption key in a certificate and issuing a password in order to limit the time for enabling decryption information and guarantee that no other user can decrypt the data.

As to claim 9, Batten-Carew discloses:

a publisher (i.e. end user) (col. 3, lines 50-52);
a trusted body (i.e. server) (col. 3, lines 35-37);

an asymmetrical key pair for a specified date and time of disclosure with an encryption key and a decryption key (col. 3, lines 39-47);
means for making the decryption key available at the specified date and time (col. 3, lines 57-61), **wherein there is a plurality of publishers, one or more asymmetrical key pairs for the specified date and time, a different asymmetrical key pair for each of the plurality of publishers** (col. 2, lines 35-37; col. 3, lines 25-28, 35-47).

Batten-Carew fails to specifically disclose:

a digital certificate signed with a private key of the trusted body, the digital certificate providing the publisher with the encryption key prior to the specified date and time;
each of the plurality of publishers has a password issued by the trusted body for preventing the disclosure of the decryption key.

Nonetheless, these features are known in the art and would have been an obvious modification of the teachings disclosed by Batten-Carew, as taught by Kudo.

Kudo discloses:

a digital certificate signed with a key of the trusted body, the digital certificate providing the publisher with the encryption key prior to the specified date and time (0003, lines 4-10; 0061, lines 10-13; 0065, lines 1-5), but does not explicitly disclose where the digital certificate is signed with a private key.

each of the plurality of publishers has a password issued by the trusted body for preventing the disclosure of the decryption key (0003, lines 4-10; 0024, lines 1-5).

It is well known in the art that signed documents in a public-key cryptography system are signed using a private key, as evidenced by Schneier (page 37, lines 26-30; page 185, lines 38-39; page 186, lines 1-7). Therefore, since Kudo discloses that the digital certificate is signed with a key, it is signed with a private key.

Given the teaching of Kudo, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Batten-Carew with the teachings of Kudo by providing an encryption key using a digital certificate prior to a specified time and issuing a password. Please refer to the motivation recited above with respect to claims 1 and 24 are to why it is obvious to apply the teachings of Kudo to the teachings of Batten-Carew.

As to claim 2, Batten-Carew fails to specifically disclose:

wherein the publisher verifies the signature on the digital certificate with the public key of the trusted body.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Batten-Carew, as taught by Kudo.

Kudo discloses:

wherein the publisher verifies the signature on the digital certificate with the key of the trusted body (0065, lines 1-5), but does not explicitly disclose where the digital certificate is verified with a public key.

It is well known in the art that signed documents in a public-key cryptography system are verified using a public key, as evidenced by Schneier (page 37, lines 26-30; page 185, lines 38-39; page 186, lines 1-7). Therefore, since Kudo discloses that the digital certificate is verified with a key, it is verified with a public key.

Given the teaching of Kudo, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Batten-Carew with the teachings of Kudo by verifying the signature on the certificate. Kudo recites motivation by disclosing that verifying the correct signature allows for the user to trust the decryption condition service provided by the time-key certificate manager (0024, lines 1-5). It is obvious that the teachings of Kudo would have improved the teachings of Batten-Carew by verifying the signature of a digital certificate in order to establish trust with the decryption condition service of the time-key certificate manager.

As to claims 3 and 12, Batten-Carew discloses:

wherein the encryption key is a public key and the decryption key is another private key in a public key infrastructure (col. 3, lines 44-47).

As to claim 4, Batten-Carew discloses:

wherein the trusted body creates the asymmetrical key pair for the specified date and time on demand from a publisher (col. 3, lines 35-40).

As to claim 5, Batten-Carew discloses:

wherein the trusted body generates one key pair for the specified date and time (col. 3, lines 35-40).

As to claim 10, Batten-Carew discloses:

including one or more recipients with means for obtaining data encrypted with the encryption key from the publisher prior to the specified date and time and means for obtaining the decryption key at or after the specified date and time (col. 3, lines 51-54, 57-61).

As to claim 11, Batten-Carew fails to specifically disclose:

wherein the certificate includes the specified date and time, the encryption key, and a name of the trusted body.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Batten-Carew, as taught by Kudo.

Kudo discloses:

wherein the certificate includes the specified date and time, the encryption key, and a name of the trusted body (0003, lines 4-10; 0005, lines 4-7).

Given the teaching of Kudo, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Batten-Carew with the teachings of Kudo by including a specified time, encryption key, and trusted body name in the certificate. Kudo recites motivation by disclosing that using a certificate guarantees that no other person can decrypt the data while limiting the time for enabling the decryption (0004, lines 4-5; 0019, lines 1-6). It is obvious that the teachings of Kudo would have improved the teachings of Batten-Carew by including a specified time, encryption key, and trusted body name in the certificate in order to limit who may decrypt the information and when the information may be decrypted.

As to claim 19, Batten-Carew discloses:

wherein the trusted body (i.e. server) is accessible by the publisher (i.e. end users) and the recipients via a communication network (col. 2, lines 35-37; col. 3, lines 50-54).

As to claim 20, Batten-Carew discloses:

a trusted body generating an asymmetrical key pair for a specified date and time of disclosure with an encryption key and a decryption key (col. 3, lines 39-47);
the trusted body providing the publisher with the encryption key prior to the specified date and time (col. 3, lines 48-49);

the publisher using the encryption key to encrypt data (col. 3, lines 50-51);

the recipient obtaining the encrypted data (col. 3, lines 51-54);

the trusted body making the decryption key available to the recipient at the specified date and time (col. 3, lines 57-61);

wherein the trusted body generates one or more asymmetrical key pairs for a specified date and time, generating a new asymmetrical key pair for each of a plurality of publishers (col. 2, lines 35-37; col. 3, lines 25-28, 35-47).

Batten-Carew fails to specifically disclose:

wherein each of the plurality of publishers has a password issued by the trusted body for preventing disclosure of the decryption key.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Batten-Carew, as taught by Kudo.

Kudo discloses:

wherein each of the plurality of publishers has a password issued by the trusted body for preventing disclosure of the decryption key (0003, lines 4-10; 0024, lines 1-5).

Given the teaching of Kudo, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Batten-Carew with the teachings of Kudo by preventing disclosure of the decryption key using a password. Please refer to the motivation recited above with

respect to claims 1 and 24 are to why it is obvious to apply the teachings of Kudo to the teachings of Batten-Carew.

3. Claims 8, 16-18, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Batten-Carew in view of Kudo as applied to claims 1, 9, and 20 above, and further in view of Di Crescenzo et al. (US Patent 6,813,358 B1 and Di Crescenzo hereinafter).

As to claims 8, 16, and 22, Batten-Carew in view of Kudo fails to specifically disclose:

wherein the decryption key is encrypted with a public key and only the recipient with a corresponding private key can obtain the decryption key.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Batten-Carew in view of Kudo, as taught by Di Crescenzo.

Di Crescenzo discloses a system and method for timed-release cryptosystems, the system and method having:

wherein the decryption key is encrypted with a public key and only the recipient with a corresponding private key can obtain the decryption key (col. 2, lines 44-45).

Given the teaching of Di Crescenzo, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Batten-Carew in view of Kudo with the teachings of Di

Crescenzo by encrypting the decryption key with a public key. Di Crescenzo recites motivation by disclosing that encrypting the decryption key allows a receiver to decrypt the data only after a release time without establishing communication between the sender and the server (col. 2, lines 17-23). It is obvious that the teachings of Di Crescenzo would have improved the teachings of Batten-Carew in view of Kudo by encrypting a decryption key with a public key in order to provide the decryption key after a release time without establishing communication between the sender and server.

As to claim 17, Batten-Carew in view of Kudo fails to specifically disclose:

wherein the trusted body has one or more agents who act on behalf of the trusted body.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Batten-Carew in view of Kudo, as taught by Di Crescenzo.

Di Crescenzo discloses:

wherein the trusted body has one or more agents who act on behalf of the trusted body (col. 2, lines 48-51; col. 4, lines 47-55).

Given the teaching of Di Crescenzo, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Batten-Carew in view of Kudo with the teachings of Di Crescenzo by using a smart card agent for the trusted body. Di Crescenzo recites motivation by disclosing that senders, receivers, and time servers may include any

computer and/or processing device such as desktop computers, portable computers, and/or smart cards in order to provide for timed-release data (col. 4, lines 40-55). It is obvious that the teachings of Di Crescenzo would have improved the teachings of Batten-Carew in view of Kudo by using a smart card as an agent in order to provide for the timed-release of data.

As to claim 18, Batten-Carew in view of Kudo fails to specifically disclose:

wherein an agent for the trusted body is a smart card having an internal clock for providing the decryption key to a recipient.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Batten-Carew in view of Kudo, as taught by Di Crescenzo.

Di Crescenzo discloses:

wherein an agent for the trusted body (i.e. server) is a smart card having an internal clock for providing the decryption key to a recipient (i.e. receiver) (col. 2, lines 48-51; col. 4, lines 47-55).

Given the teaching of Di Crescenzo, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Batten-Carew in view of Kudo with the teachings of Di Crescenzo by using a smart card agent for the trusted body. Please refer to the motivation recited above with respect to claim 17 as to why it is obvious to apply the teachings of Di Crescenzo to the teachings of Batten-Carew in view of Kudo.

(10) Response to Argument

Claims 1, 9, 20, 23, and 24

It is argued by the Appellant that the teachings of Batten-Carew and Kudo fail to disclose of *multiple publishers that each have a password issued by a trusted body for preventing disclosure of a decryption key.*

The Appellant argues that Kudo is directed to providing an encryption key to a user, as contrasted with a decryption key, passworded or otherwise. The Appellant also argues that the examiner cannot ignore the plain meaning of the term 'password' and that Kudo does not teach the use of a password that prevents disclosure of the decryption key.

The examiner respectfully disagrees with the Appellant's assertion. Kudo discloses that the system can be used as an electronic safe system when the information user is replaced by a bank (i.e. recipient) and the information server is replaced by a depositor (i.e. publisher), where the time-key manager (i.e. trusted body) transmits to a depositor (i.e. publisher) a time-key certificate that includes disclosure time information and a public key for encryption (0062, lines 1-7). In this instance, it is obvious that the bank will have more than one depositor, therefore displaying a plurality of depositors (i.e. publishers) that each have a relationship with the bank and time-key manager. It is noted that the Appellant's claims do not provide further description of the password or how it is used to prevent disclosure of the decryption key. It is also noted that the Appellant's claims describe that the decryption key is transmitted from the

trusted body to the recipient, and not to the publisher, which is issued the password. Therefore, the examiner has interpreted the password to include any information that relates to controlling the distribution of the decryption key. Kudo discloses that when the correct signature (i.e. password) of the time-key certificate manager (i.e. trusted body) is included in the time-key certificate, the decryption condition service provided by the time-key certificate manager can be trusted (0024, lines 1-5), and the decryption key is transmitted to user A (i.e. recipient) when the decryption conditions are met (0020, lines 10-12). Further, Kudo discloses that the time-key manager issues a time-key certificate to User B (i.e. publisher); therefore, each publisher is issued a signature (i.e. password) in a time-key certificate. Since this signature must be correct for the decryption condition service (i.e. provision of the decryption key to a recipient) to be trusted, the signature (i.e. password) is related to the distribution of the decryption key.

The Appellant also argues that the digital signature of Kudo is the digital signature of the certificate authority that provides a public encryption key for an intended message recipient, and not a particular user.

The examiner respectfully disagrees with the Appellant's assertion. It is noted that the feature upon which applicant relies (i.e., digital signature is of a particular user) is not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Sarah Su/

Examiner, Art Unit 2431

Conferees:

/Christopher A. Revak/

Primary Examiner, Art Unit 2431

/William R. Korzuch/

Supervisory Patent Examiner, Art Unit 2431